The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
02/20/2012

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

1. Firefox versions prior to 19.0
2. Firefox Extended Support Release (ESR) versions prior to 17.0.3
3. Thunderbird versions prior to 17.0.3
4. Thunderbird Extended Support Release (ESR) versions prior to 17.0.3
5. SeaMonkey versions prior to 2.16

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

1. Large and medium business entities: **High**
2. Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

- Miscellaneous memory safety hazards (MFSA 2013-21)?Several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products have been identified. Some of these bugs showed evidence of memory corruption under certain circumstances, and some of these could be exploited to run arbitrary code.

- Out-of-bounds read in image rendering (MFSA 2013-22)?This issue is caused when performing an out-of-bounds read while rendering GIF format images. This could cause a non-exploitable crash and could also attempt to render normally inaccessible data as part of the image.
- Wrapped WebIDL objects can be wrapped again (MFSA 2013-23)?A wrapped WebIDL object can be wrapped multiple times, overwriting the existing wrapped state. This could lead to an exploitable condition in rare cases.
- Web content bypass of COW and SOW security wrappers (MFSA 2013-24)?It is possible to bypass some protections in Chrome Object Wrappers (COW) and System Only Wrappers (SOW), making their prototypes mutable by web content. This could be used leak information from chrome objects and possibly allow for arbitrary code execution.
- Privacy leak in JavaScript Workers (MFSA 2013-25)?The file system location of the active browser profile was available to JavaScript workers. While not dangerous by itself, this could potentially be combined with other vulnerabilities to target the profile in an attack.
- Use-after-free in nsImageLoadingContent (MFSA 2013-26)?There is a use-after-free issue in nsImageLoadingContent when content script is executed. This could allow for arbitrary code execution.
- Phishing on HTTPS connection through malicious proxy (MFSA 2013-27)?This issue allows for a spoofing of addresses that can be used for phishing attacks by fooling users into entering credentials, for example.
- Use-after-free, out of bounds read, and buffer overflow issues found using Address Sanitizer (MFSA 2013-28)?There is a series of use-after-free, out of bounds read, and buffer overflow problems rated as low to critical security issues in shipped software. Some of these issues are potentially exploitable, allowing for remote code execution

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

1. Upgrade vulnerable Mozilla products immediately after appropriate testing.
2. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
3. Do not open email attachments or click on URLs from unknown or untrusted sources.
4. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/?

http://www.mozilla.org/security/announce/2013/mfsa2013-21.html

http://www.mozilla.org/security/announce/2013/mfsa2013-22.html
http://www.mozilla.org/security/announce/2013/mfsa2013-23.html
http://www.mozilla.org/security/announce/2013/mfsa2013-24.html
http://www.mozilla.org/security/announce/2013/mfsa2013-25.html
http://www.mozilla.org/security/announce/2013/mfsa2013-26.html
http://www.mozilla.org/security/announce/2013/mfsa2013-27.html
http://www.mozilla.org/security/announce/2013/mfsa2013-28.html